Training Material

We make sure

PY-INS
Exercise 07O KVM Switch – Installation

Issue January 2008
Version V.7.12.01.01
Pages 41

CONTENT

1 Preface:

In this Exercise, you will learn how to configure a FSC KVM switch (digital model: S3-1621).

2 Conventions

- = This symbol points out hazards that can lead non-functional configurations, data loss, equipment damage or even personal injury

- Text… = This symbol followed by smaller text highlights important background information and tips

- 2.3.4 = These numbers refer to steps that you must carry out in order to continue with the procedure

- *Italics* = Commands, menu items, names of buttons, options, variables, file names and path names

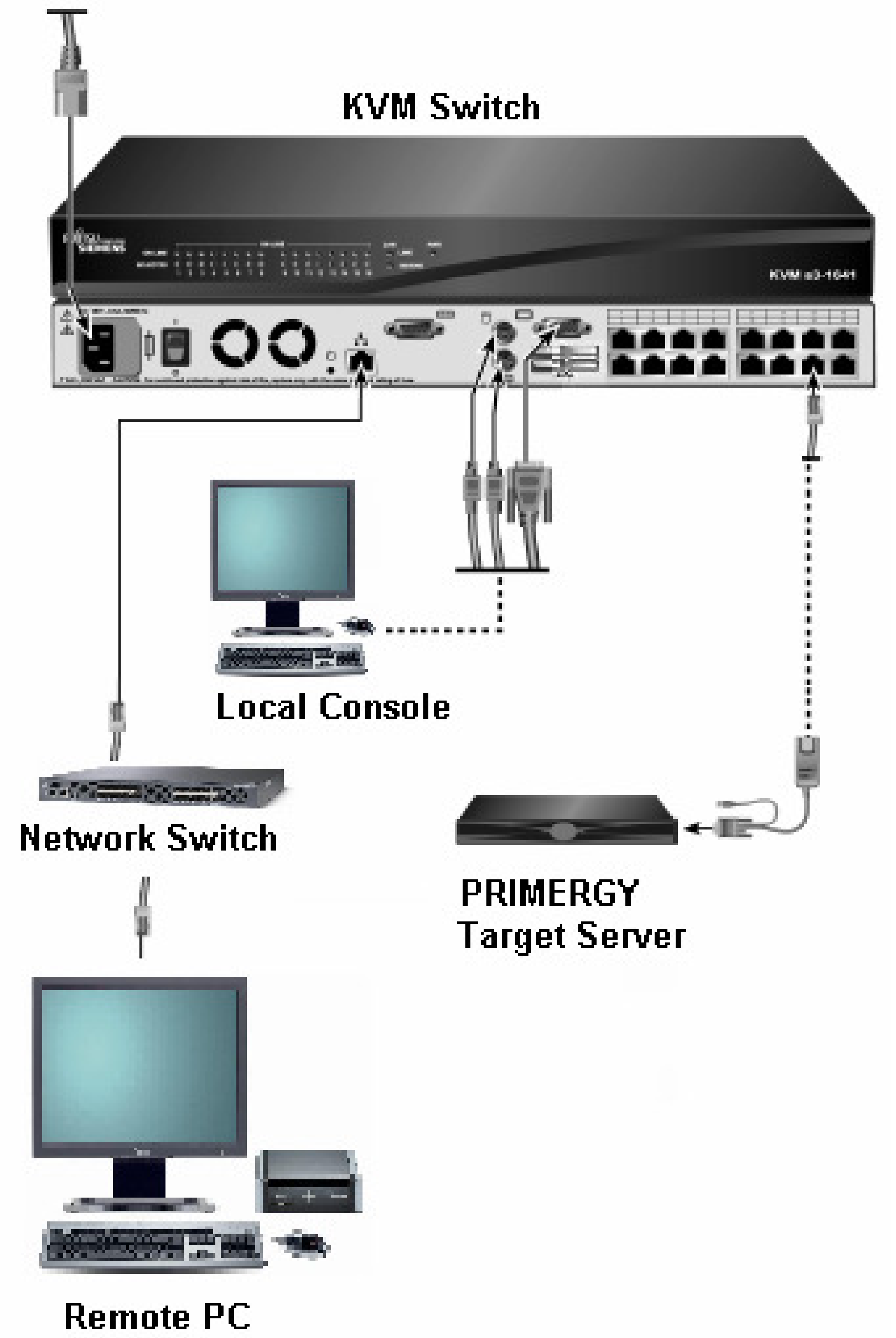
- <abc> = Angle brackets are used to enclose variables which are to be replaced by actual values

- `fixed font` = Screen output

    - [Key] = Square brackets represent keys on the keyboard. If capital letters are to be entered explicitly, then the Shift key is shown, e.g. [Shift] - [A] for A. If two keys need to be pressed at the same time, then this is shown by placing a hyphen between the two key symbols

3 KVM Switch Basic Installation

3.1 Objective



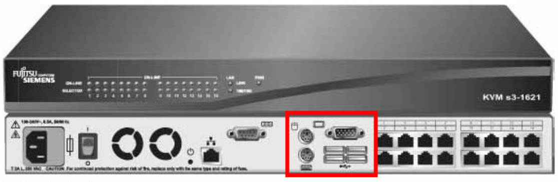
3.2 Requirements and Prerequisites

- Note: Some types, sizes and numbers might vary from the ones shown in the screen-shots.

3.2.1 Switch: KVM s3-1621

- The KVM s3-1621 appliance has user peripheral ports for PS/2, USB, keyboards and mice.
- Additionally, virtual media, such as generic removable media and CD drives, can be connected to any one of four USB ports

(Please have patience till capture 5)



KVM s3-1621

1

3.2.2 Local Console

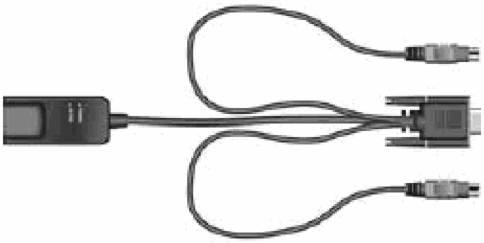
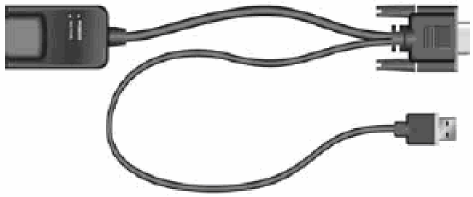
- for configuring the KVM switch on-site
- Monitor, PS/2 or USB keyboard and mouse



2

3.2.3 KVM-IA Intelligent Adapters

- In general you can use the following KVM-IAs with the KVM s3-1621, but for our Exercise we only need the first and second cable:

3.2.3.1 KVM S2-Adapter PS/2-VGA **PS/2 and VGA connectors**	 3
3.2.3.2 KVM S3-Adapter USB2-VGA **USB2 and VGA connectors** → required for virtual-media Connections (see capture 6)	 4
3.2.4 Target Device: Primergy Server e.g. RX100 S4	 5
3.2.5 Network Switch e.g. Cisco MDS9124	 6
3.2.6 PC running with a running remote software KVM s3 e.g. an Esprimo Q running the **KVM** s3 Client	 7

3.3 Installation Steps

3.3.1 Step 1: Connecting power to the switch

- Power down all servers that will be part of your switching system.
- Locate the power cord that came with the switch.
- Plug one end into the power socket on the rear of the switch and the other end into an appropriate AC wall outlet



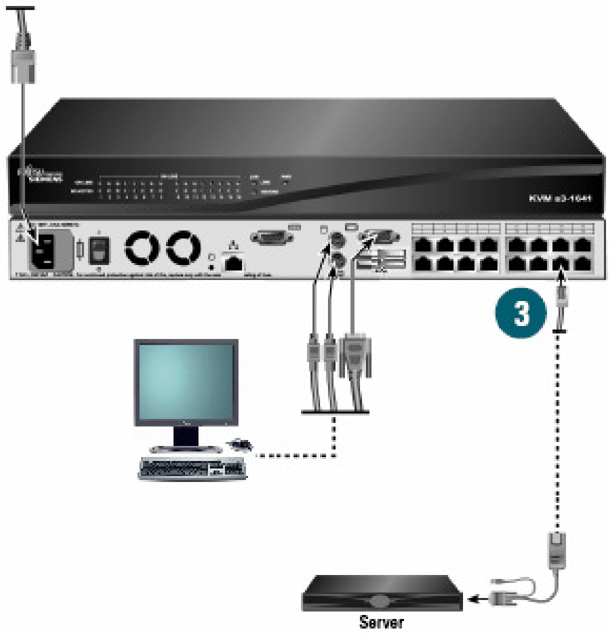
3.3.2 Step 2: Connecting the local port

- Plug your VGA monitor, PS/2 or USB keyboard
- Plug the mouse cables into the appropriately labeled switch ports.



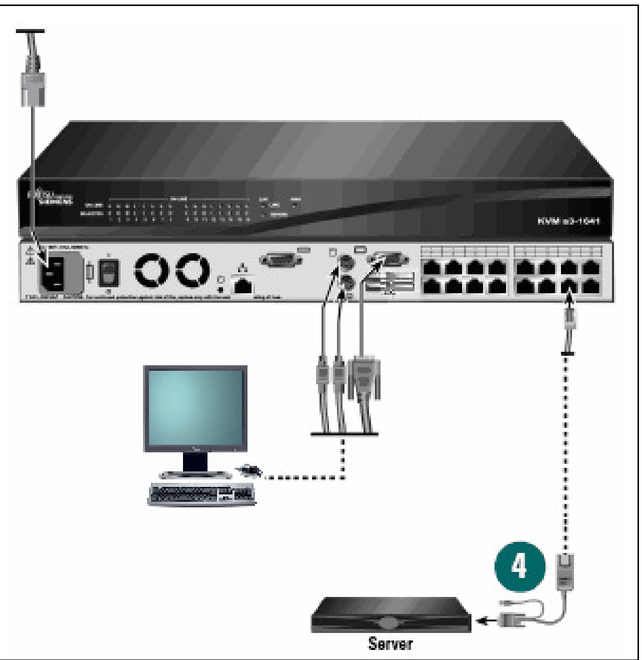
3.3.3 Step 3: Connecting a KVM-IA to the switch

- Choose an available port on the rear of your switch.
- Plug one end of a CAT 5 cable (4-pair, up to 10 meters) into a numbered port and plug the other end into the RJ-45 connector of a KVM-IA.



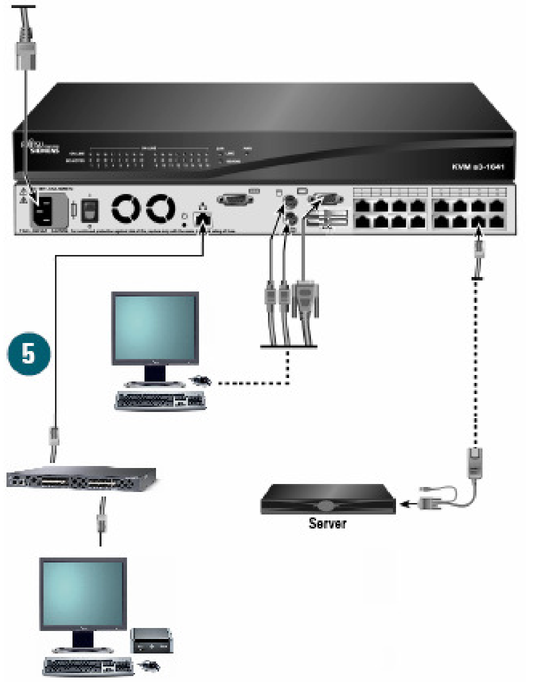
3.3.4 Step 4: Connecting a server to the KVM-IA

- Plug the KVM-IA into the appropriate ports on the back of the server.
- Repeat this procedure for all servers that are to be connected to the switch.



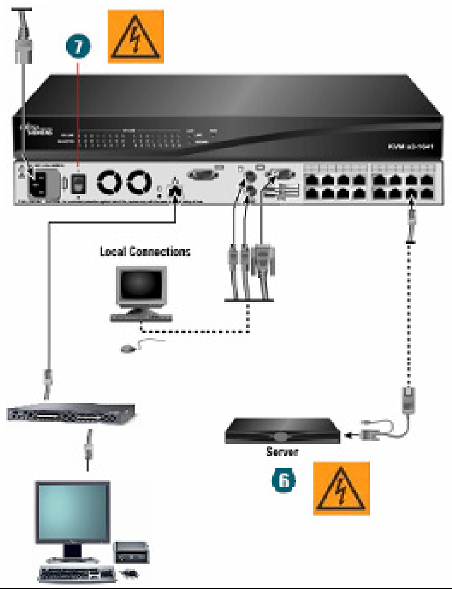
3.3.5 Step 5: Connecting network and remote users

- Plug a CAT 5 cable from your Ethernet network into the LAN connector on the back of your switch.
- Connect your remote PC to the Network
- Network users will gain access through this port.



3.3.6 Step 6 + 7: Powering up target server and switch

- Power up the **target server** <u>and then</u>
- power up the **switch.**



4 Basic Operations

- In this section you will learn how to control the Switch (KVM s3-1621) system from the local console

4.1 Local Console

- The **local console** uses analog ports to connect keyboard, monitor, and mouse
- You can get access to all **Basic Operations** threw the **OSCAR** interface



4.2 Start the Oscar Interface

- To start the **OSCAR** interface, please press one of the following buttons:

  → Press 1 x "**Print Screen**"

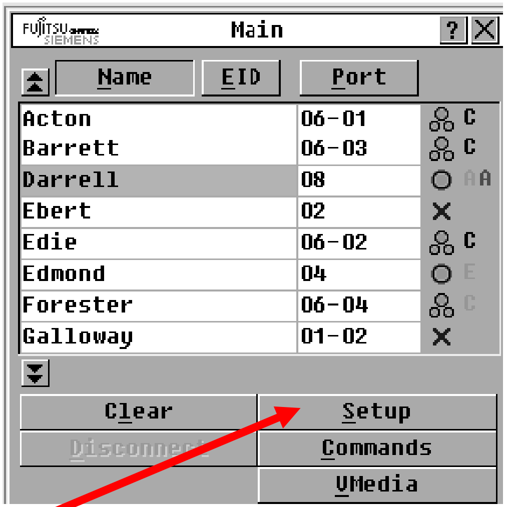
  -or-

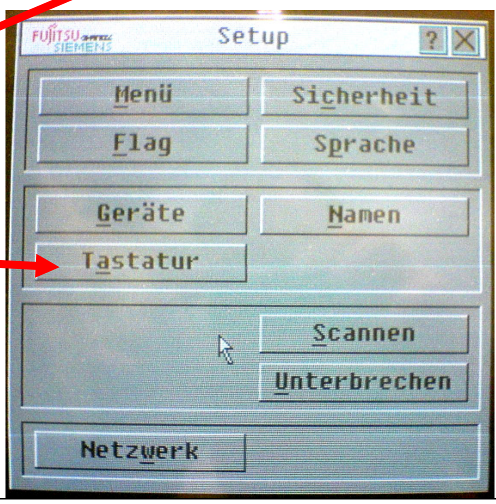
  →Press 2 x "**Control**" or "**Alt**" or "**Shift**" (twice within 1 second)

- To change the key sequences that can be used to start the **OSCAR interface**, please

  →Press "Setup"

  →Press "Keyboard"





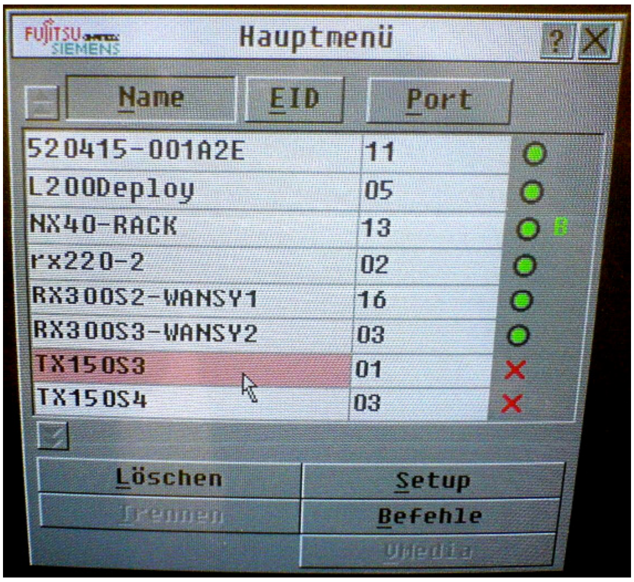
4.3 Changing Names

- Devices can be identified by <u>customizable</u> names

- To change this <u>customizable</u> names click

→Setup

→Names



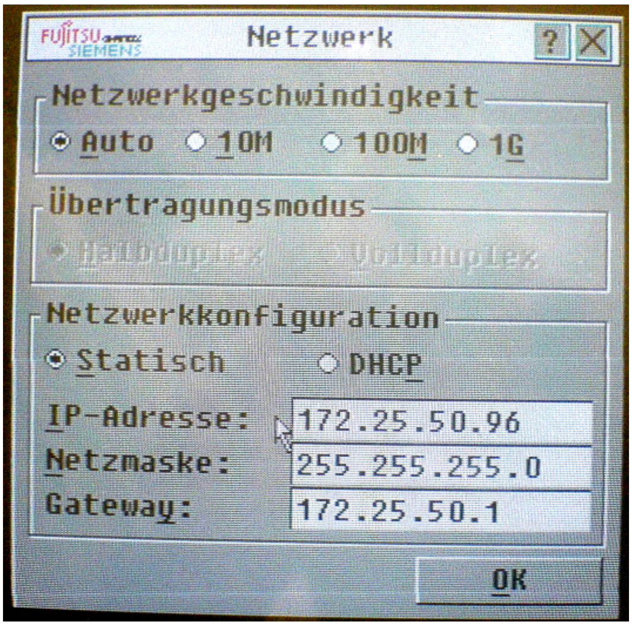


4.4 Changing the IP-Adress the KVM

- To change the <u>customizable</u> **IP-Adress** click in the **Setup menue**:

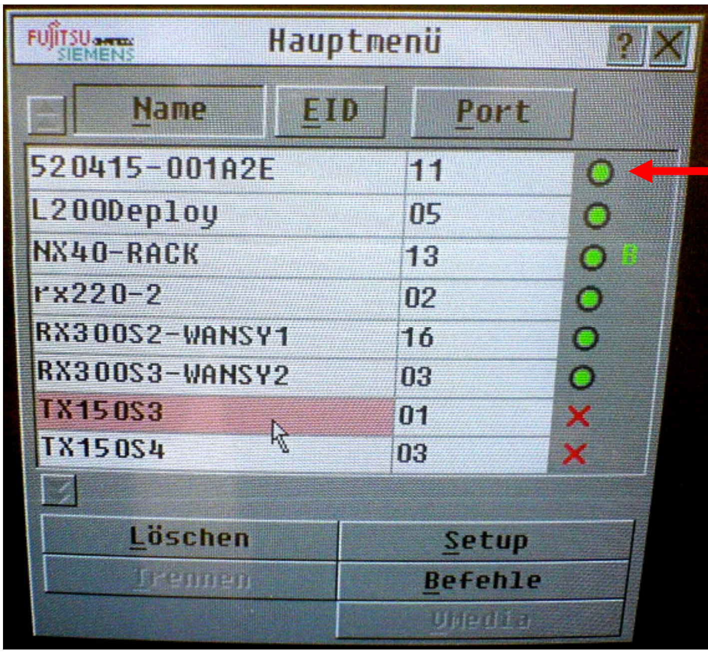
→Network

→customize the <u>IP-Adress of the KVM switch</u> and configure your network-settings as you need



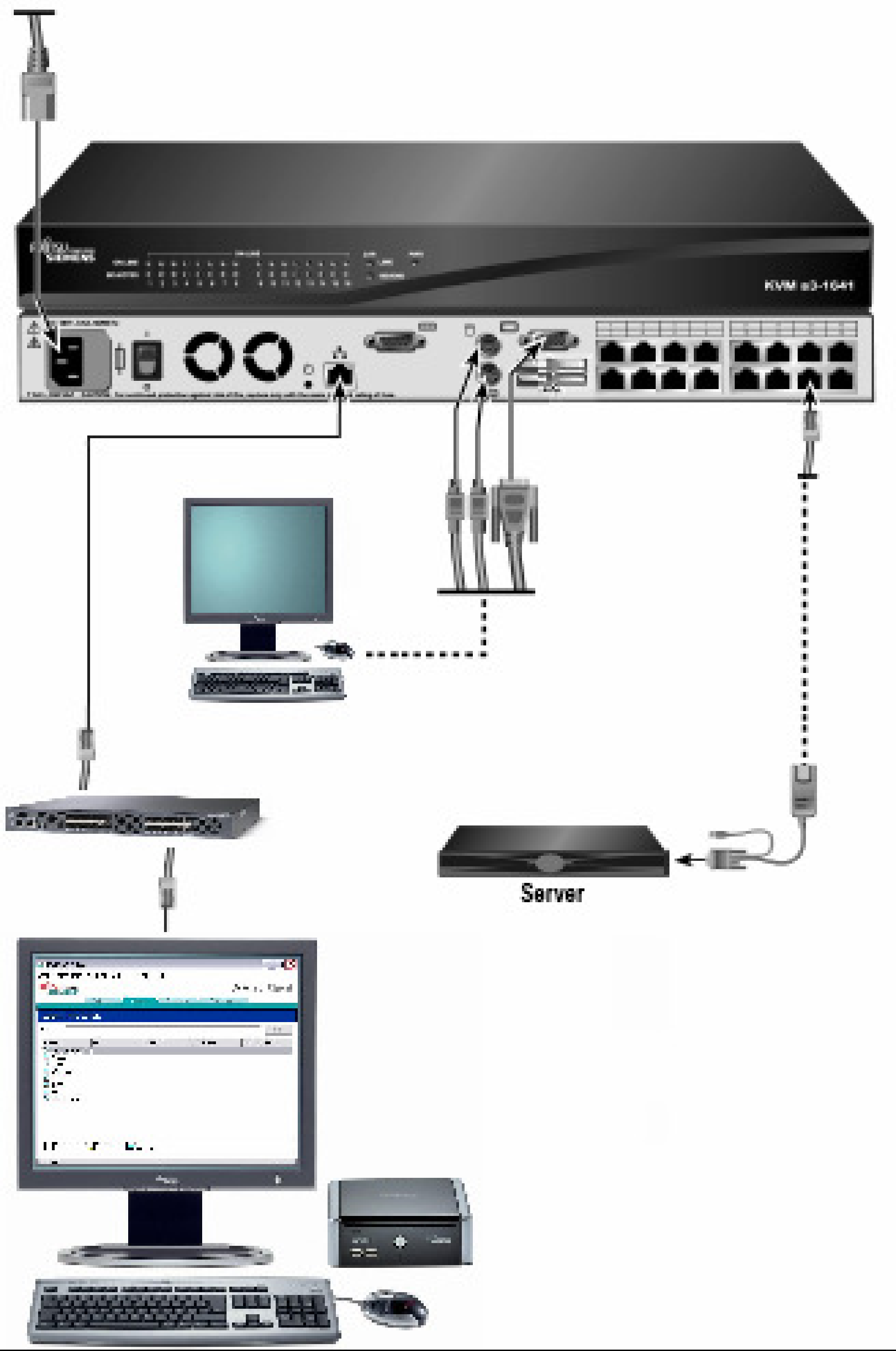
4.5 The Status Symbols in the Main Menue

Description	Symbol
The KVM-IA is online (green circle).	
The KVM-IA is offline or is not operating correctly.	
The target device is tiered through an earlier appliance model. The target device and the earlier appliance model is online and has power.	
The target device is tiered through an earlier appliance model. The earlier appliance model is offline or does not have power.	
The KVM-IA is being upgraded (yellow circle). When this symbol is visible, do not turn off and turn on the appliance or connected target devices and do not disconnect the KVM-IA. Doing so might damage the KVM-IA permanently.	
The KVM-IA is being accessed by the indicated user channel (green channel letter).	A
The KVM-IA is blocked by the indicated user channel (black channel letter). For instance, in Figure 8 on page 17, user C is viewing Forester, but is blocking access to Acton, Barrett, and Edie which are connected to the same KVM-IA.	A
A virtual media connection is established to the target device connected to the indicated user channel (blue letter).	I



5 Using the Remote Software: KVM s3 Client

5.1 Objective



5.2 Remote Software: KVM s3 Client

- Users get access to the **KVM s3-1621** and all attached **target devices** through the Ethernet from a remote PC. This client can be anywhere if a valid network connection exists.

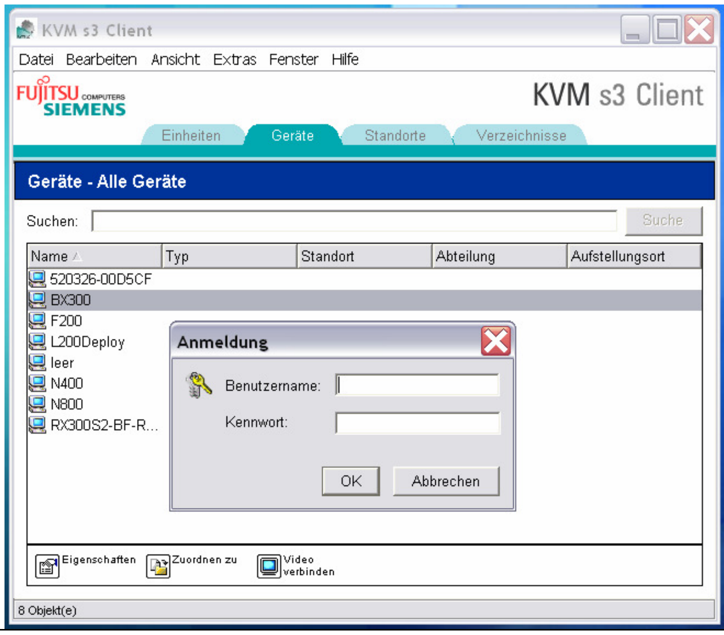
- The remote Software installed on the remote computer is called **KVM** s3 Client



- After you started the KVM s3 Client, a catalogue of all target devices, for which you have permission to manage, will be listed.

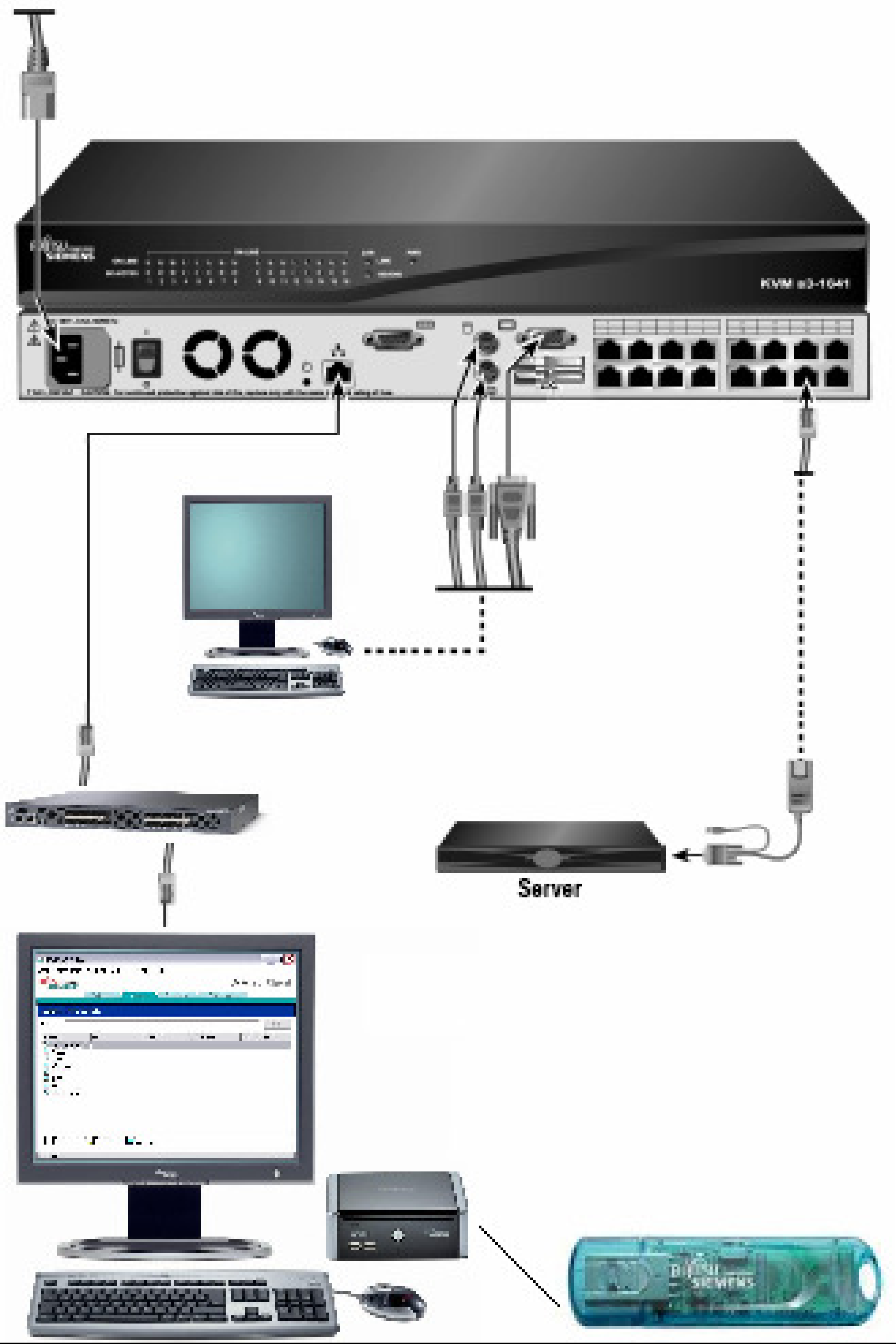
- Please login if necessary with:

- username:
- password:



6 Virtual Media

6.1 Objective

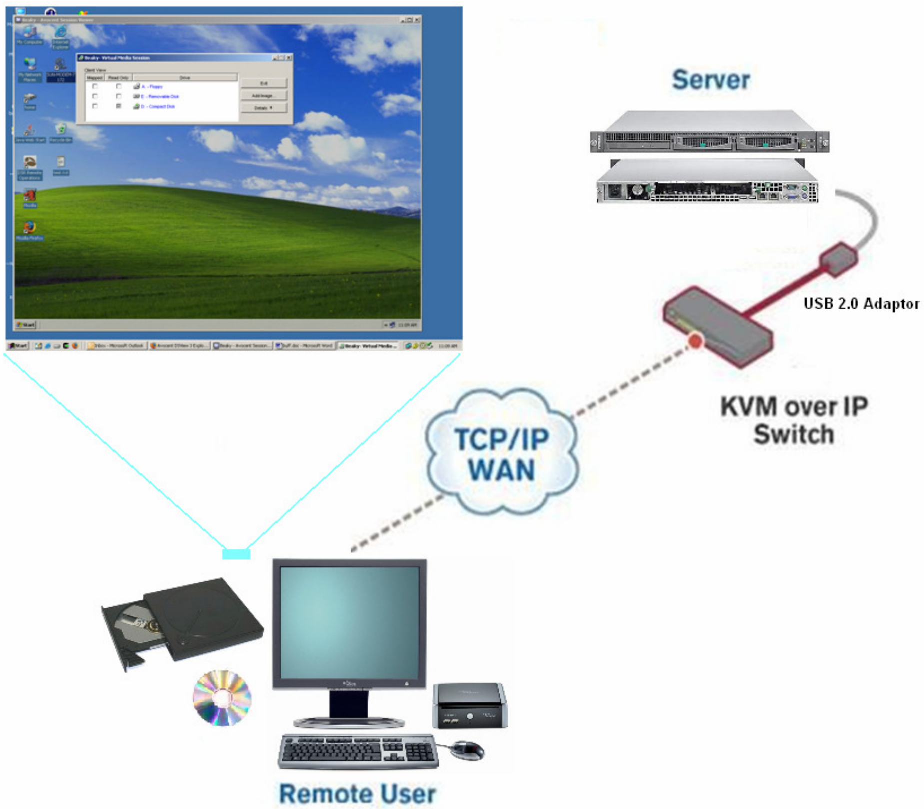


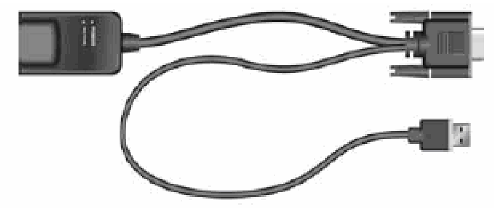
6.2 Connectable Virtual Media

- Users could connect any kind of conventional media through the Ethernet from the remote PC.
- VM enables remote loading of:
  - Floppy
  - USB Flash Drives
  - ISO image
  - CD-ROM



- The KVM s3-1621 appliances support virtual media when connected to a KVM-IA.
- Virtual media can be connected directly to the KVM s3-1621 using one of four USB ports on the KVM s3-1621
- Additionally virtual media can be connected to <u>any</u> remote workstation that is running the KVM s3 Client



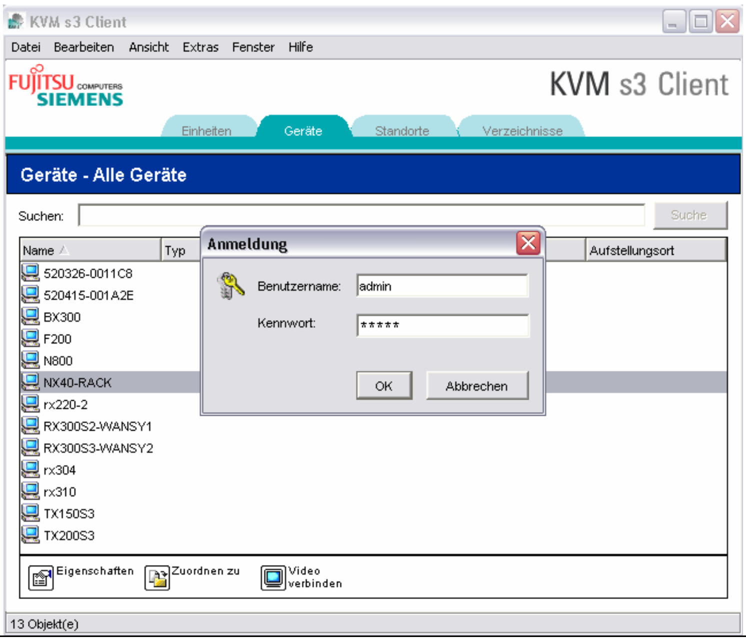
• The remote workstation has to be connected to the KVM s3-1621 using an Ethernet connection using a KVM s3-Adapter USB2-VGA cable. • **KVM S3-Adapter USB2-VGA USB2 and VGA connectors**	

6.3 Virtual media restrictions

- The KVM s3 Client supports only mapping of USB 2.0 (1.1) Floppy-drives and Flash.



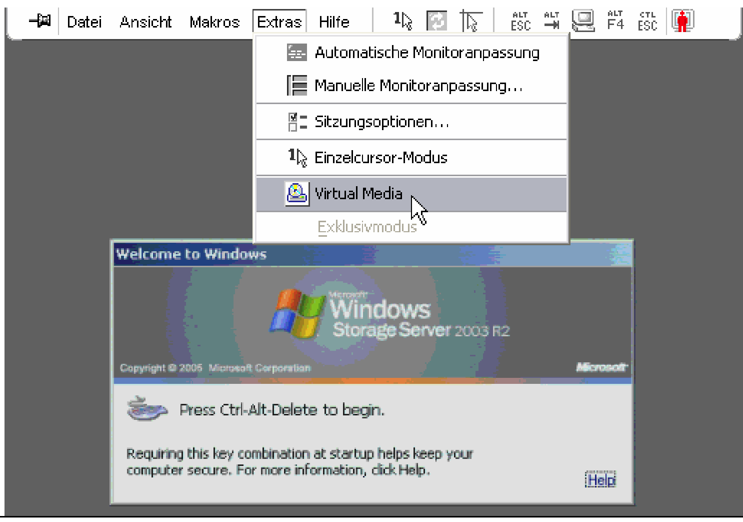
6.4 Logon to a PRIMERGY with a KVM S3 dongle



6.5 Open Virtual Media configuration scrren

Extras → Virtual Media

: Virtual Media is only available if an KVM S3 donlge is connected



6.6 Connect an Image

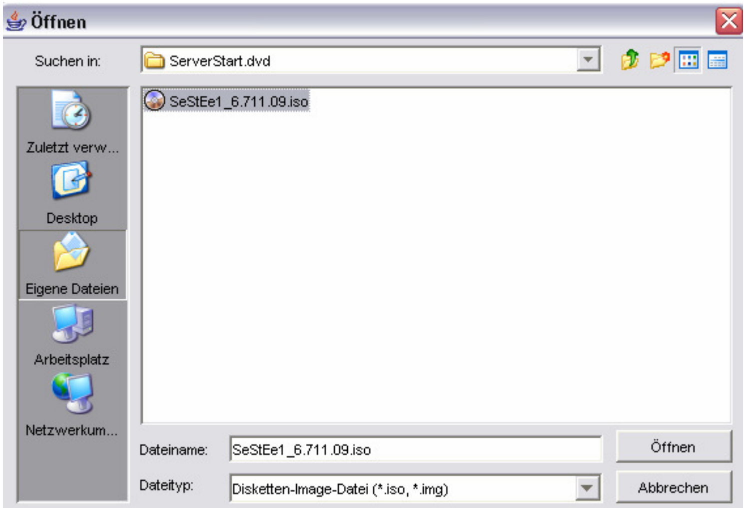
add an Image



6.7 Choose an Image

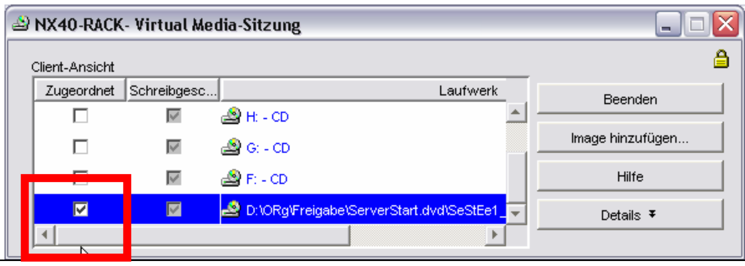
Select

[\\192.168.xx.200\download\Serverstart\SeStEe1_6.711.09.iso](\\192.168.xx.200\download\Serverstart\SeStEe1_6.711.09.iso)



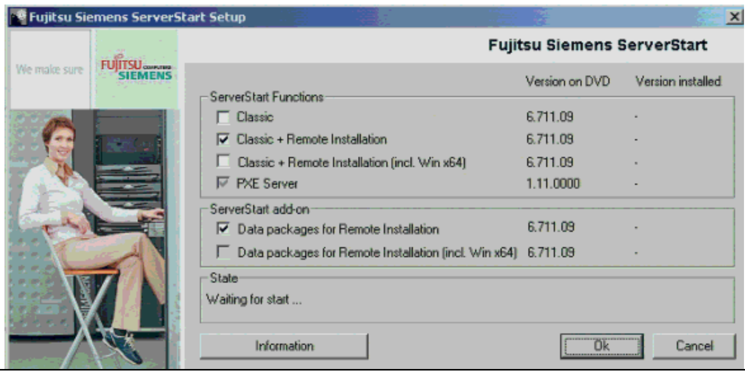
6.8 Connect it

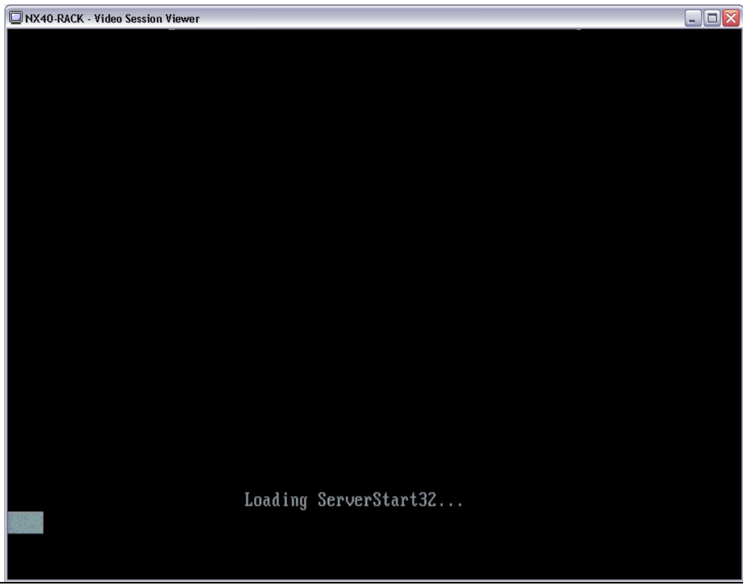
And leave the windows open



6.9 Serverstart installation sxcreen appears

Press cancel



6.10 Restart the server	
6.11 Press F12 or change the boot order on your Server	
6.12 The server boot the ServerStart image local	
6.13 Disconnect the device Or wait until boot is finished	

7 Optional Exercise: LDAP & AD (Lightweight Directory Access Protocol & Active Diretory)

- The KVM solution of Fujitsu Siemens Computers can be integrated with **LDAP** / **AD** without any need to change the schema of the directory.

- There are three main ways to configure access authentificaton via LDAP:

1. **Basic** mode
2. **Attribute** mode
3. **Group** mode

- **Basic mode** will authenticate the user for **AD**, but will give **full access** to both, KVM switch and servers, to any authenticated user.

- **Attribute mode** will give access to any user configured, based on the text entered in the "info"-box. This box is placed in the **AD settings** for the **user**. The info field can be set to the following three levels of access:

  - **KVM Appliance Admin**
  - **KVM User Admin**
  - **KVM User**

- **Group mode** is the final and most advanced way of configuring access. The group mode gives the most options for configuring security; the focus of this training is on the Group mode.

7.1 Overview

Operations	Appliance administrator	User administrator	User
Preempt other users	All	Equal and lesser	No
Set network and global values	Yes	No	No
Reboot and upgrade firmware	Yes	No	No
Manage user accounts	Yes	Yes	No
Monitor target device status	Yes	Yes	No
Access target devices	Yes	Yes	Assigned by Admin

7.2 Configuring Groups

a) The KVM switch is given a useful name under the SNMP settings in the AMP (Appliance Management Panel).

b) The IA (Integrated Access) cables are given names to match the AD entries for their respective servers. Servers which lack an AD entry, such as Linux servers, are given new computer accounts in AD to represent them.

c) A user for browsing the AD domain is created in AD.

d) An OU for containing the KVM security groups is created in AD

e) The information of the DC, including IP, LDAP port and the user account created in step 3 are entered under the LDAP settings in the AMP.

f) A new, global security group is created in the OU created in step 4.

g) The relevant users and servers are added to the security group.

7.3 Practical guide: Group mode - LDAP / AD setup

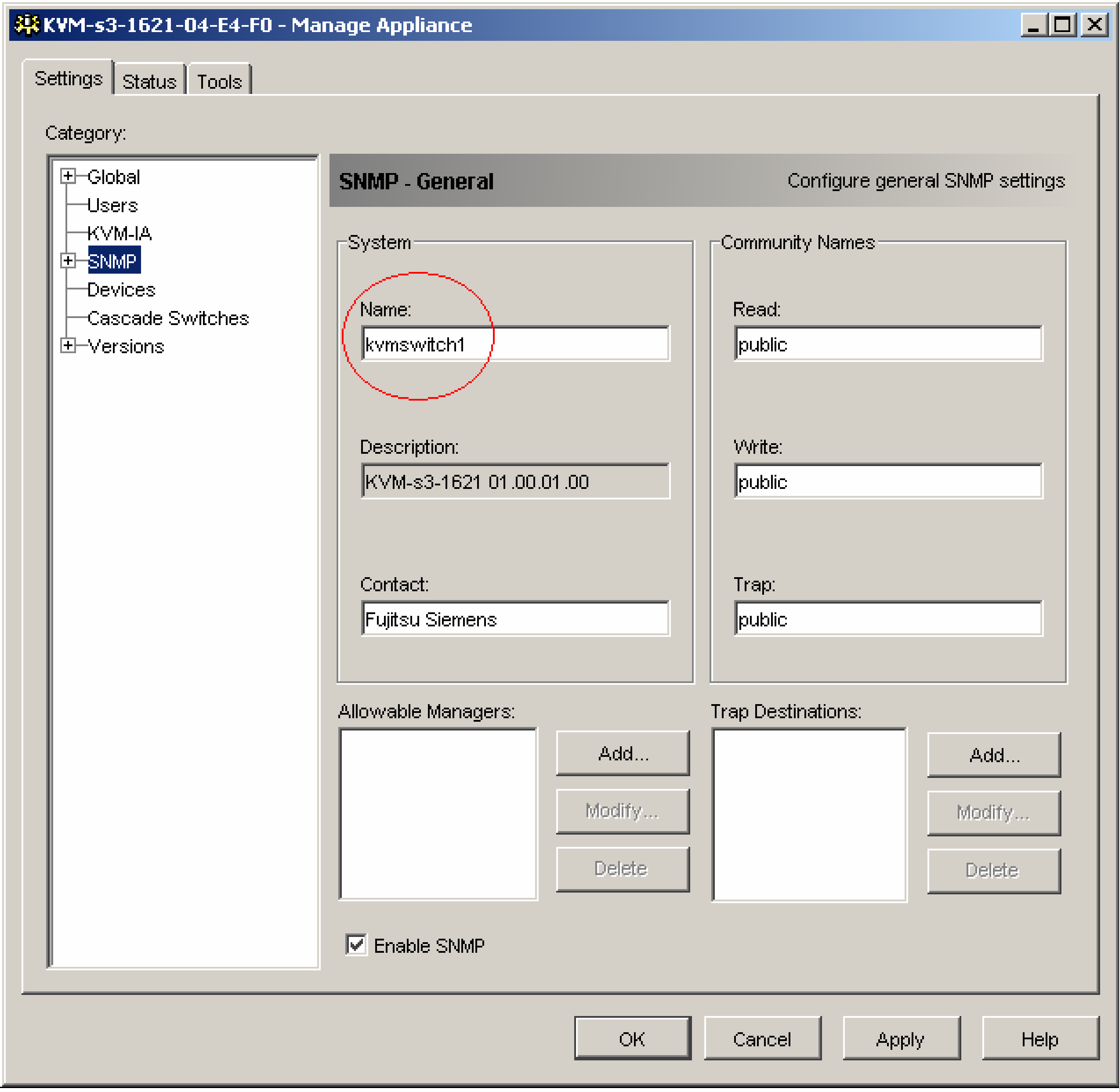
7.3.1 Renaming the KVM switch

a) Please give the KVM switch a **reasonable name**, you can find this option under the **SNMP settings** in the **AMP** (Appliance Management Panel).

b) The **default name** of the switch is: **the switch type** + **last numbers of the MAC address**. As this is hard to remember, **it makes no sense to keep the default name.**

c) Set the Name to KVMSwitchxx (xx is your Group name)

d) **Power cycle** the KVM switch after applying these settings.



7.3.2 Renaming the IA cables (servers)

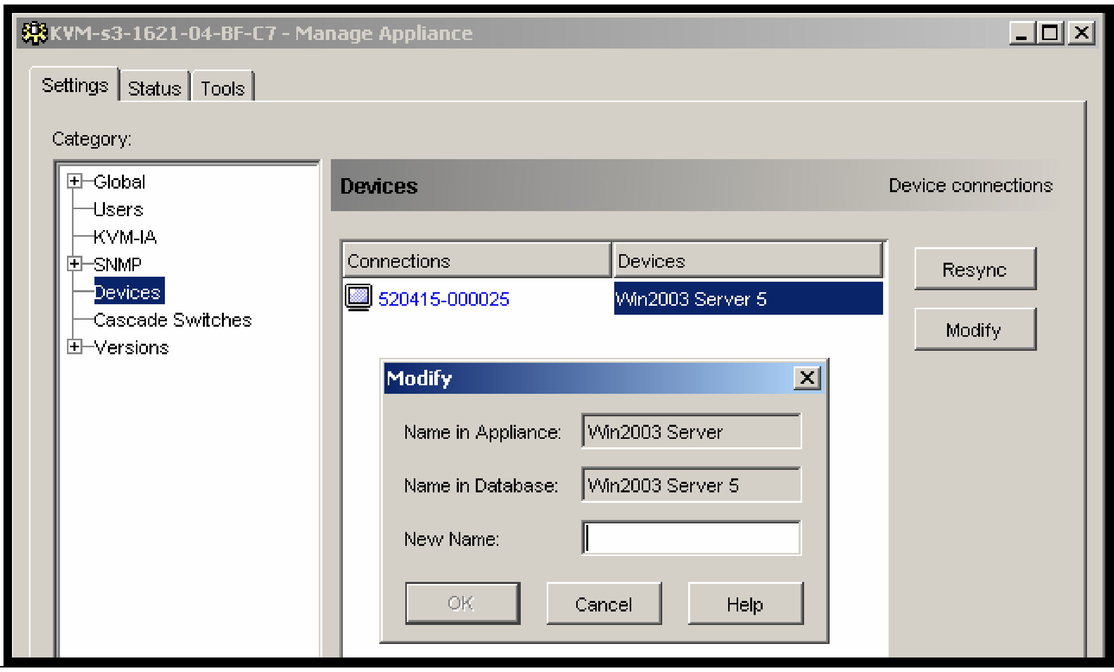
7.3.2.1 Notes

- **The IA cables (Integrated Access) are given names <u>to match</u> the Active Directory (AD) entries for their respective servers.**
- **LINUX: Servers which lack an AD entry, such as <u>Linux servers, are given new computer accounts in AD to represent them.</u>**
- **It is important that the IA cable names and the names in AD match <u>exactly</u>.**

7.3.2.2 Renaming

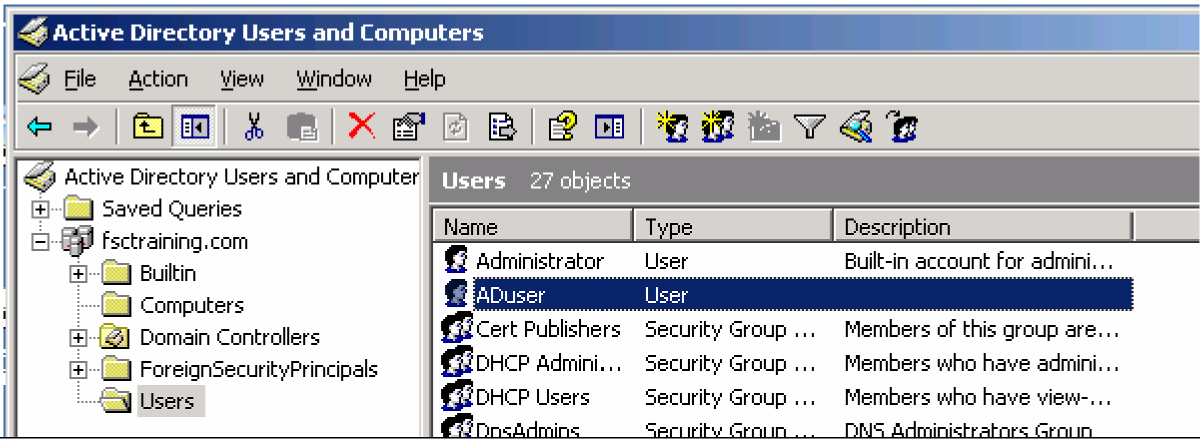
1. AMP **(Appliance Management Panel)**
2. **Click** "Devices**" and then choose the device to change** (**highlighting)**
3. **Click** "Modify" **to open the dialog box where the name can be changed.**
4. "Apply" **changes.**
5. Close the **AMP**.

- **NOTE: The renaming of servers can also be done from the local analog port through the OSCAR by clicking "Setup" and then "Names".**



7.3.3 Creation of user to browse AD

a) Create a normal **User** for browsing the Active Directory in the Active Directory.
b) Named ADuser with password fsc (check the account with you configuration plan or ask the teacher)



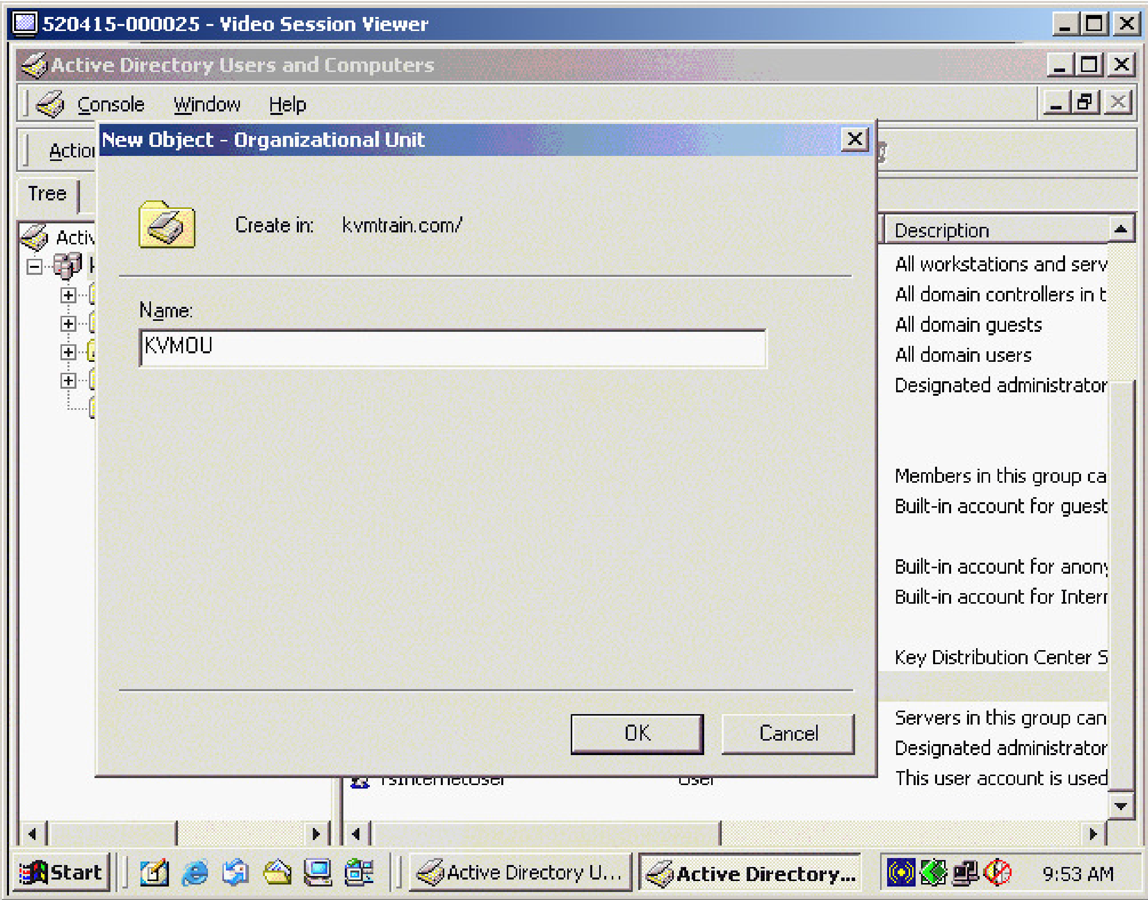
7.3.4 Creation of a security group to govern access

a) Create an **Organisation Unit** for containing the KVM **security groups** in the **Active Directory**

Nomaly this has been done by your teacher !

b) The **Organisation Unit** can be located inside transaction nested **Organisation Units**.

- Transaction nesting **of up to three levels has been confirmed to work with. Please note that an** Organisation Unit **should be created in the root domain in AD.**



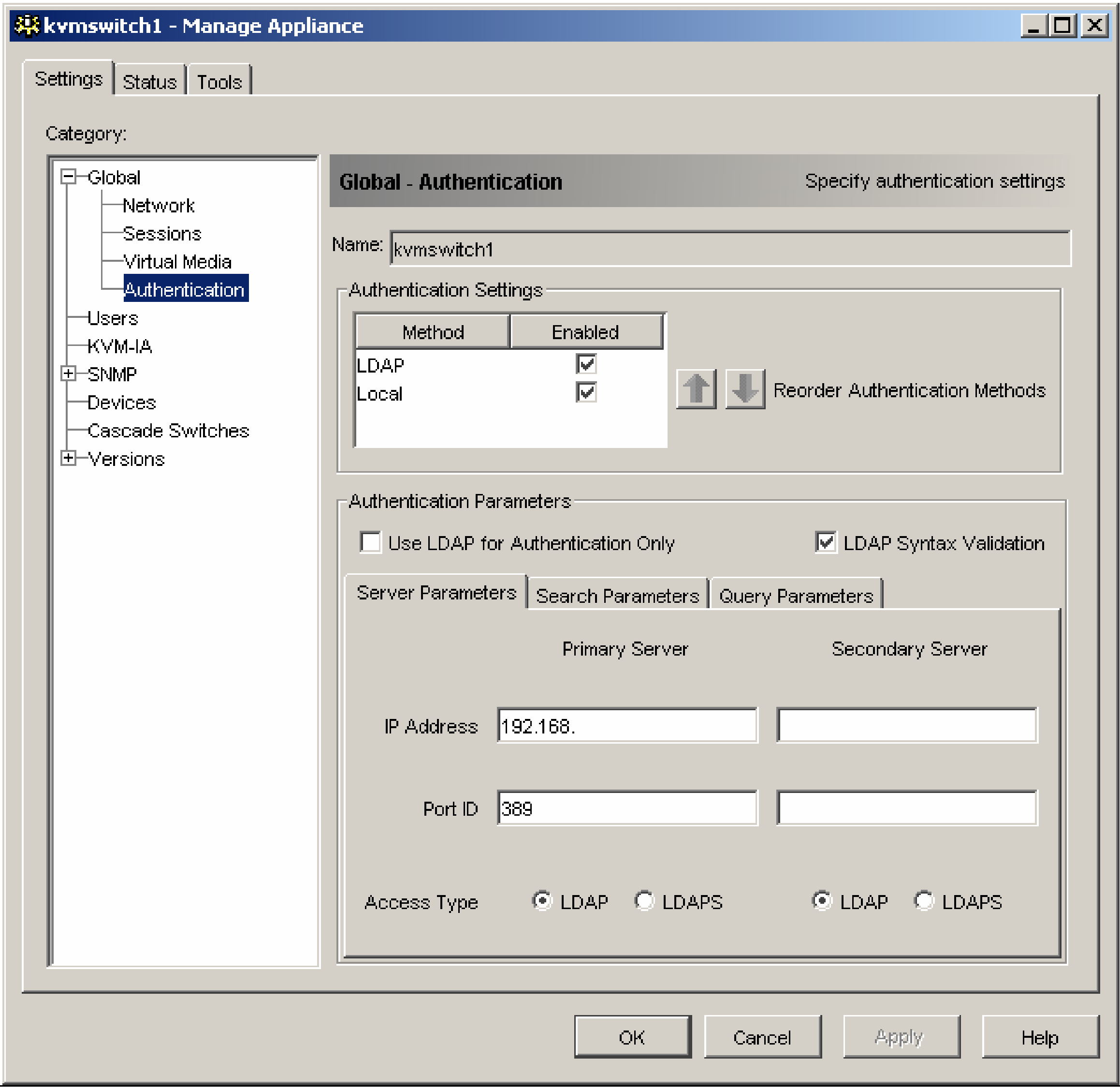
7.3.5 Configuration of LDAP settings in the AMP

Tab 1: Server Parameters

1. Enable **LDAP** by **checking the checkbox** in the the **Authentification Settings**

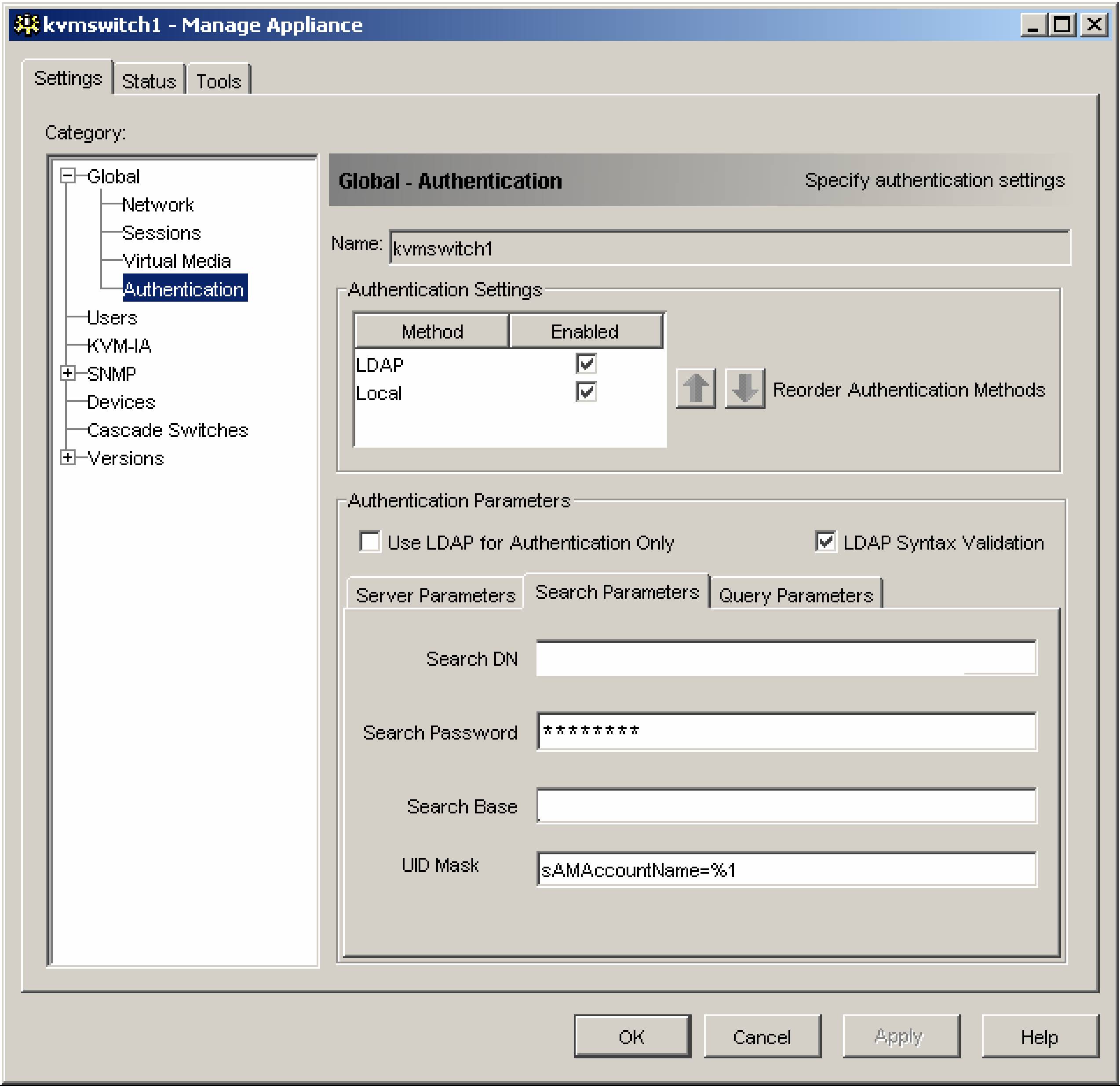
2. Enter the **DC IP address**. 192.168.xx.200 (check your configuration plan or ask the teacher)

3. Select **LDAP**



Tab 2: Search Parameters

1. Enter on the next tab "**Search Parameters"** the information for the user to browse the directory.
2. The "**Search Base**" should be set to the root domain of the forest.
3. you can use the LDAPBrowser tool for testing purpose \\192.168.xx.200\download\LDAPBrowser



Search DN: CN=ADuser,DC=fsctraining,DC=com

Search Password =fsc (or use the configuration plan)

Search Base : CN=Users,DC=fsctraining,DC=com

UID=SamAccountName=%1

Tab 3: Query Parameters

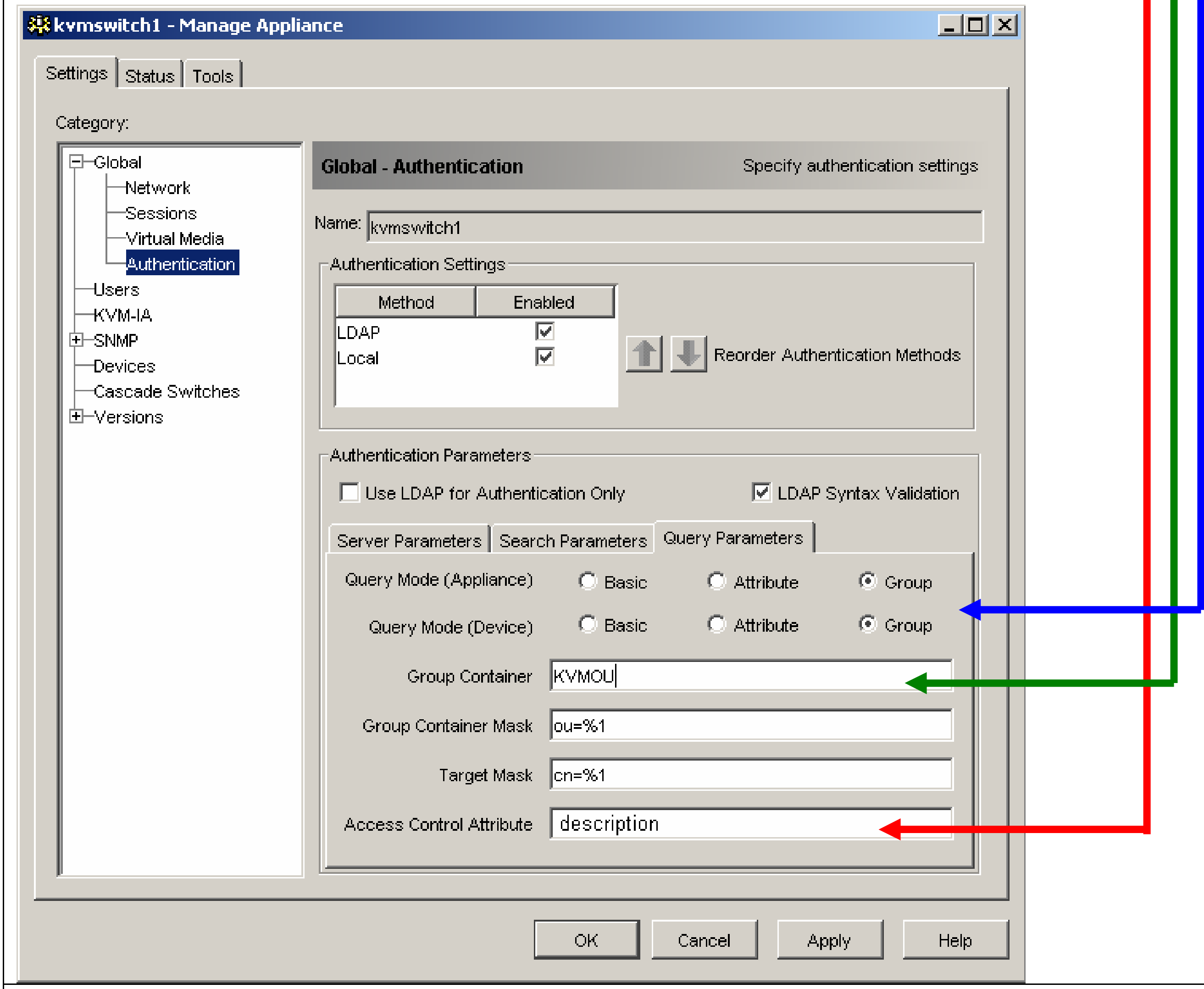
1. Set both **Query Mode** option button to the value **Group**.

2. Type in **KVMOU**

3. The other parameters don't have to be changed for **Active Directory** normally

4. The item **Access Control Attribute** is in use to avoide modifying the **Active Directory scheme.**

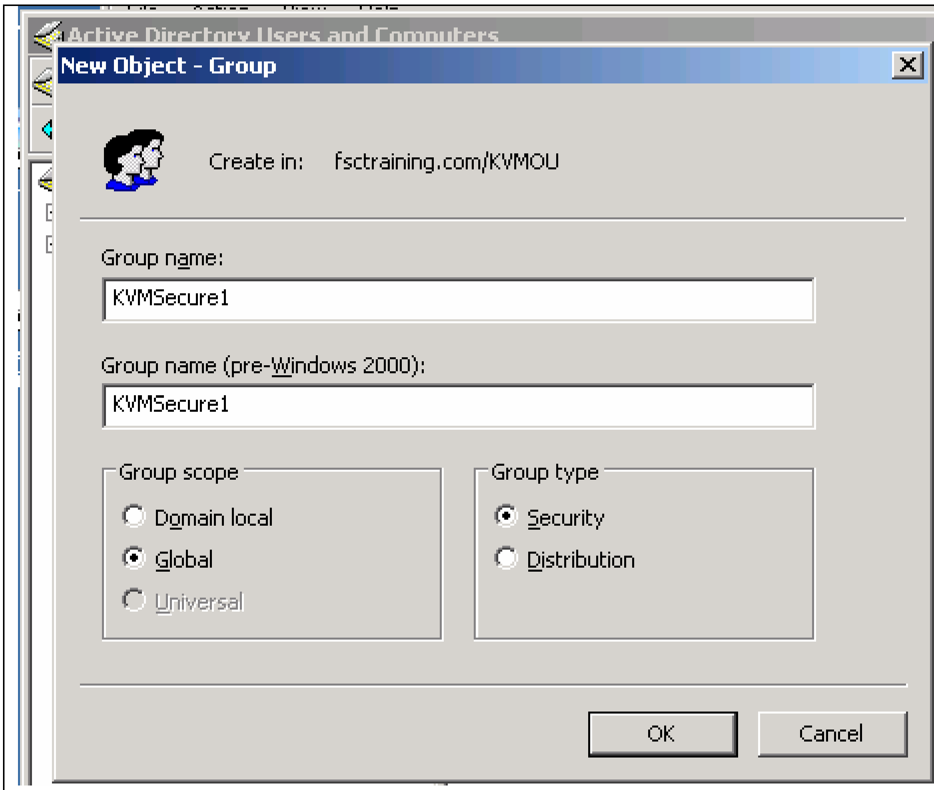
Access Control Attribute: description



7.3.6 Creation of an Organisation Unit to hold the security groups

1. Create a new, global security group "KVMSecure" in the **Organisation Unit** created in chapter 7.3.4

i Nomaly this Domainconfiguration has been done by your teacher!



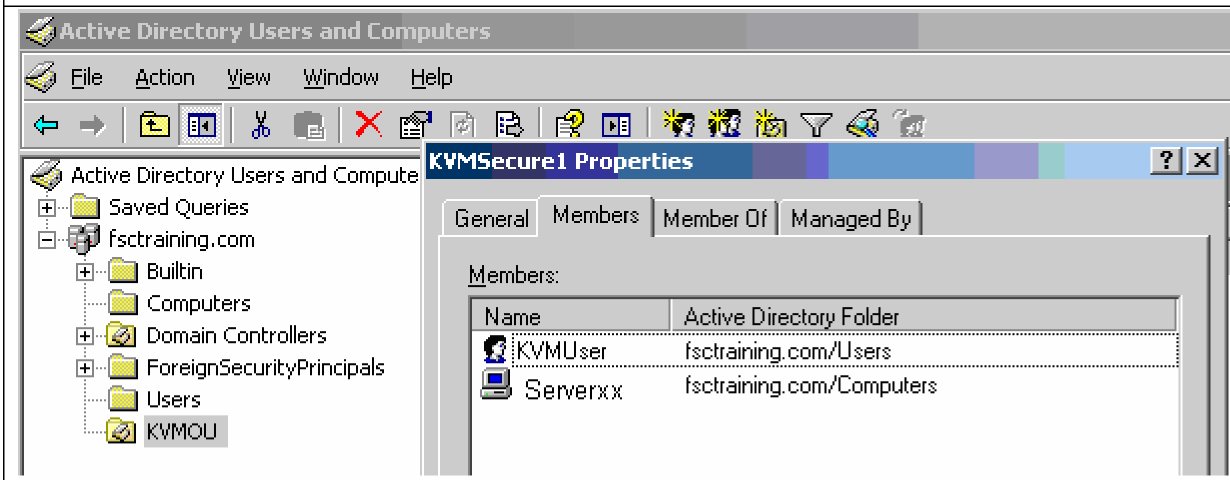
7.3.7 Adding users and servers to the security group

- The relevant users and servers are added to the security group

1. Select the users you want to have access.
2. Select the serversxx and user "serverxx" into the new security group.

- **Note: Servers without Active Directory accounts**

  Not all servers will have an account in **Active Directory**. This is true for **Linux and Unix** based servers and also for the **KVM switches**. Therefore, in order to govern access to KVM switches and other appliances / servers not listed in **Active Directory** it is necessary to create new Computer accounts for these devices. They can be created anywhere as long as the user for browsing AD has access to reading their entries. For the KVM switches it may make sense to put the Computer accounts in the new **Organisation Unit** together with the security groups.



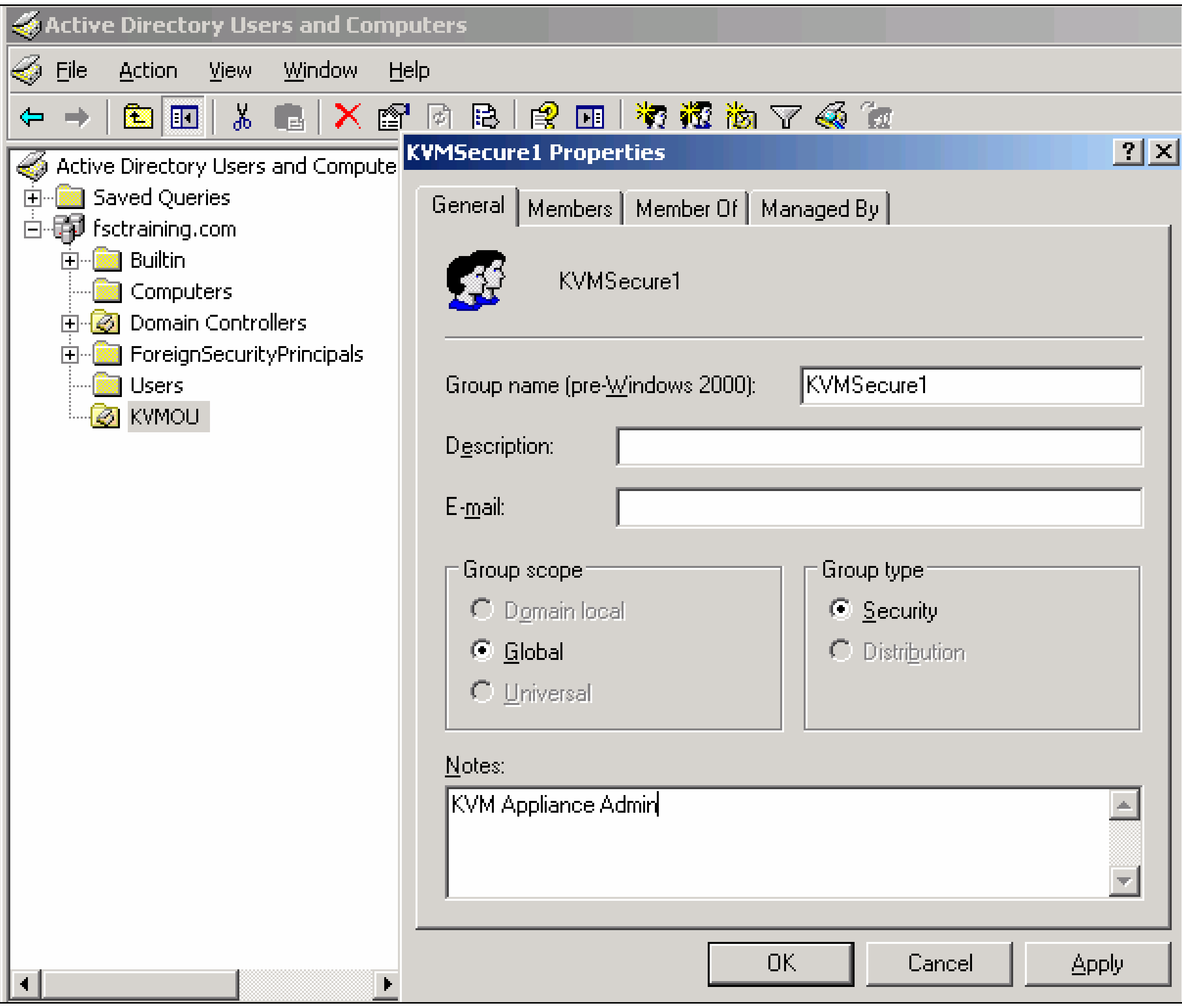
➢ **Note: Adding the access control attribute**

Now the security group has to be marked as containing either KVM Users, KVM User Admins or KVM Appliance Admins. The differences between the levels of access are shown in capture 9.1. and below, because the access levels are the same as for **Attribute Mode** access.

However, the advantage of **Group mode** is that groups can be assigned on a group basis, giving more granular access. Please note that this is mainly useful for KVM switch access, as long as all of them have server access by default.

Operations	Appliance administrator	User administrator	User
Preempt other users	All	Equal and lesser	No
Set network and global values	Yes	No	No
Reboot and upgrade firmware	Yes	No	No
Manage user accounts	Yes	Yes	No
Monitor target device status	Yes	Yes	No
Access target devices	Yes	Yes	Assigned by Admin

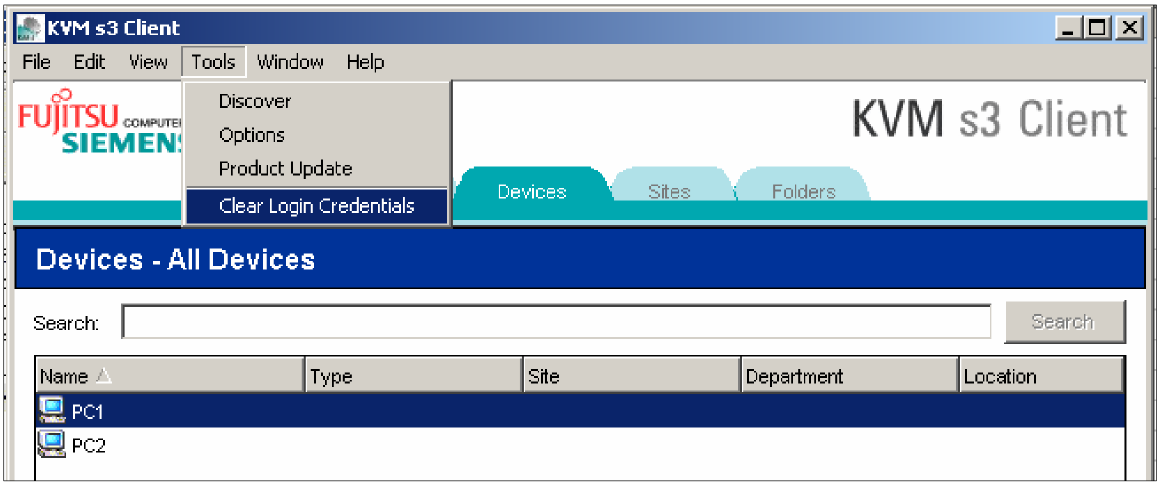
7.3.8 Configuration of the textbox called "Notes" ("info" field)



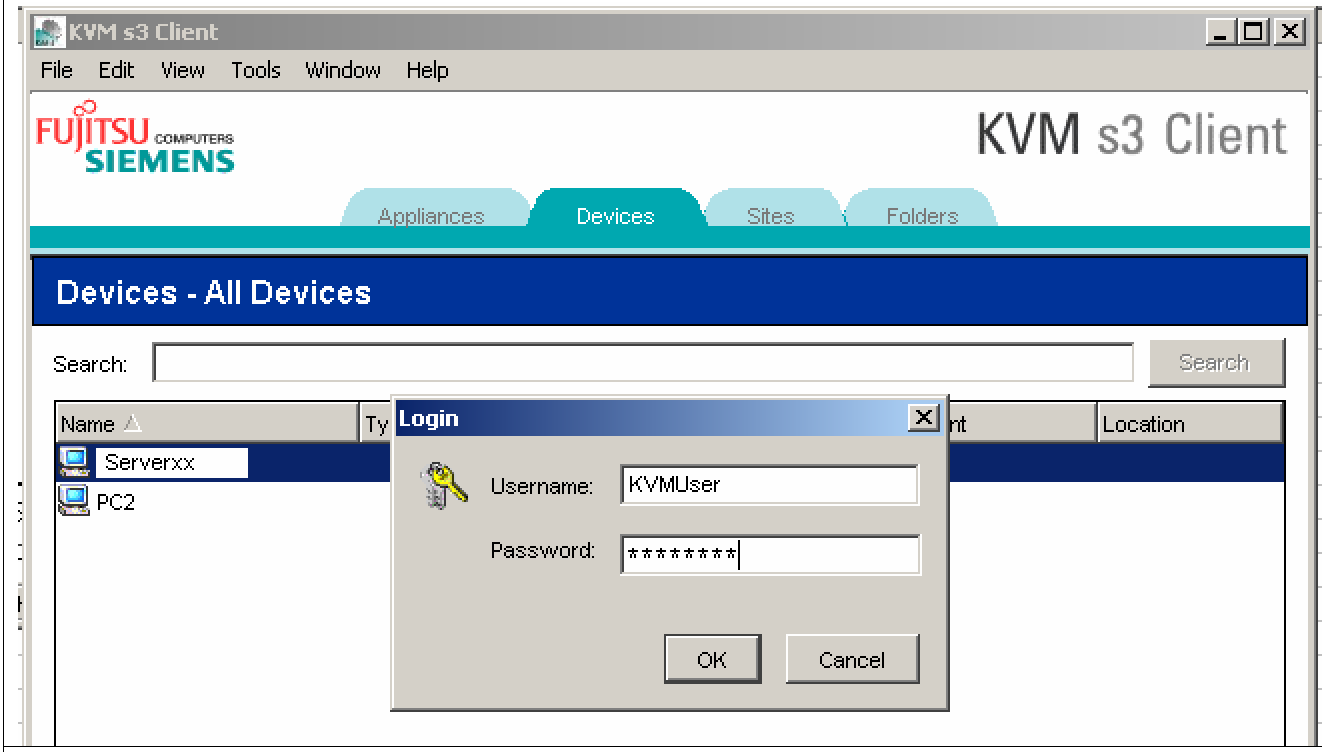
7.3.9 Testing the configuration

➢ Now everything should be configured and it's time for a test to ensure the correct working.

1. Clear the **logon credentials** in the s3-Client as follows:



2. Double click on a server of the security group.
3. Log in.
4. There is no need to specify the domain when logging in, so in our example we will use "KVMUser" rather than KVMUser@fsctraining.com



- The **server screen** should be pop up after a few seconds of delay. If any errors appear, please go back and make sure the configuration is correct. The KVM switch can also be debugged from the serial console in case more detailed error information is needed

8 Optional Exercise: Password Recovery

8.1 Setting or change a password

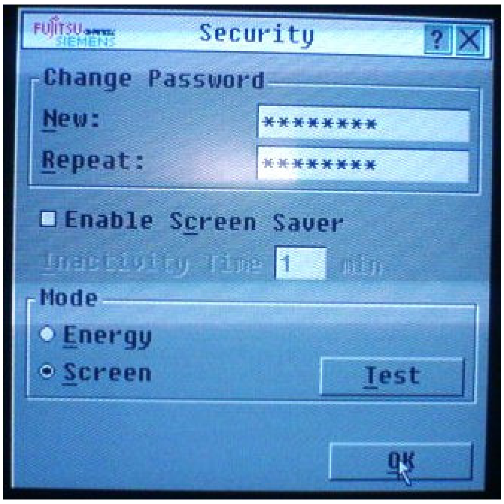
- Press “Print Screen”
- Click **Setup** in the **Main** window

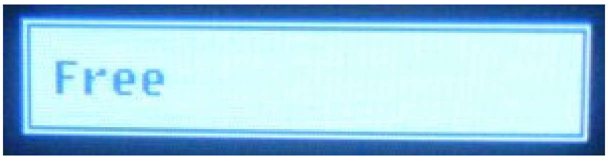


- Click **Security.** If a password is already set, the Password window opens



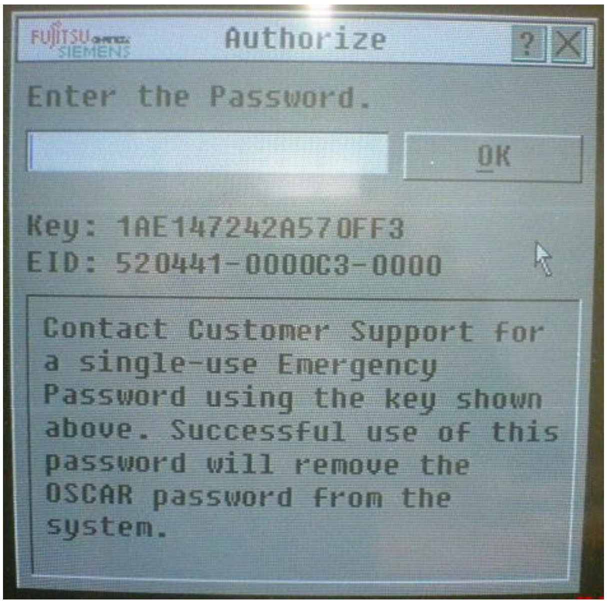
- Type the password and click **OK**.
- Double-click the New field.
- In the **New** field, type the new password.
- In the **Repeat** field, type the password again.
- Click **OK.**



## 8.2 Recovering a password	
1. **Power cycle** the appliance (this will take about 45 seconds).	
2. At the "**Free**" prompt, press **Print** Screen	
3. The Authorize window appears.	
4. Click the **Forgot Password** button at the bottom of the Authorize window.	

The following information appears:

- A 16 digit HEX key (example - **1234ABCDFFFF7890**)
- The EID for the appliance (example - **123456-000001-1234**)
- Instructions to contact **FSC Customer Support**



5. Keeping the Authorize window open

6. Contact FSC Customer Support to **request a** single use, **emergency password**.

To obtain the emergency password, you will have to provide the 16 digit HEX key and the EID for the appliance. **FSC Customer Support** will return a 16 digit HEX emergency password.

7. Enter the 16 digit HEX emergency password (case sensitive) in the Authorize menu.

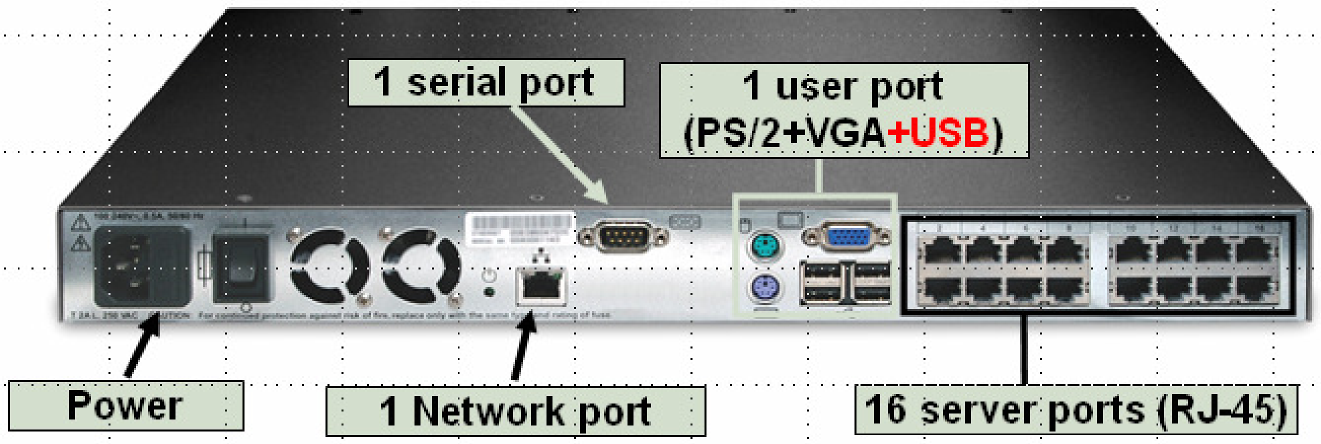
8. Click **OK**.
   - The Main window appears, with password security now disabled. You now have full access to the appliance via the OSCAR menu.

9. Create a new password to re-enable security, if desired, or let it free



9 Optional Exercise: Upgrading the Firmware

9.1 Objective

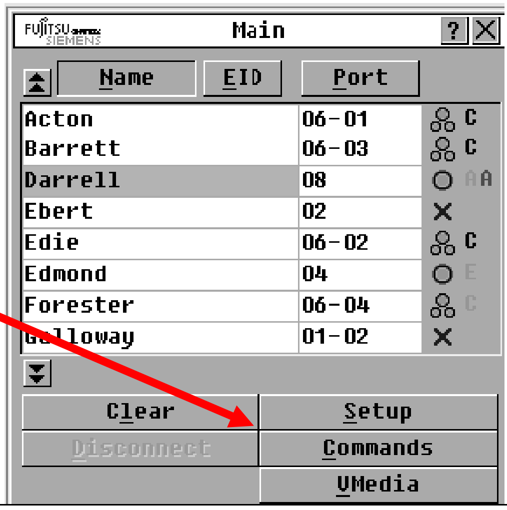


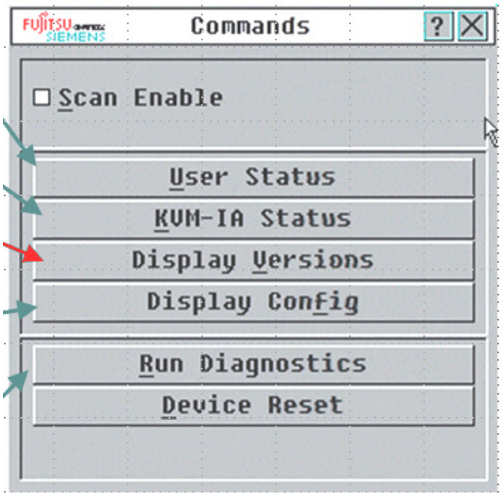
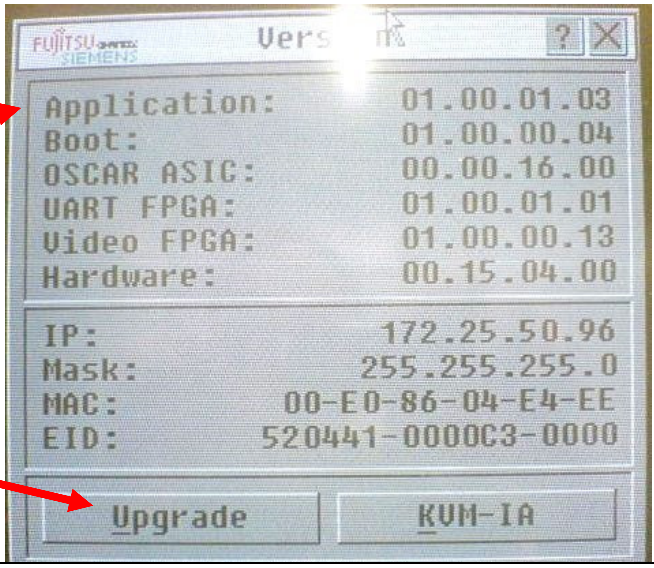
➢ Note: The serial port is used for firmware upgrades

9.2 Displaying Version Information

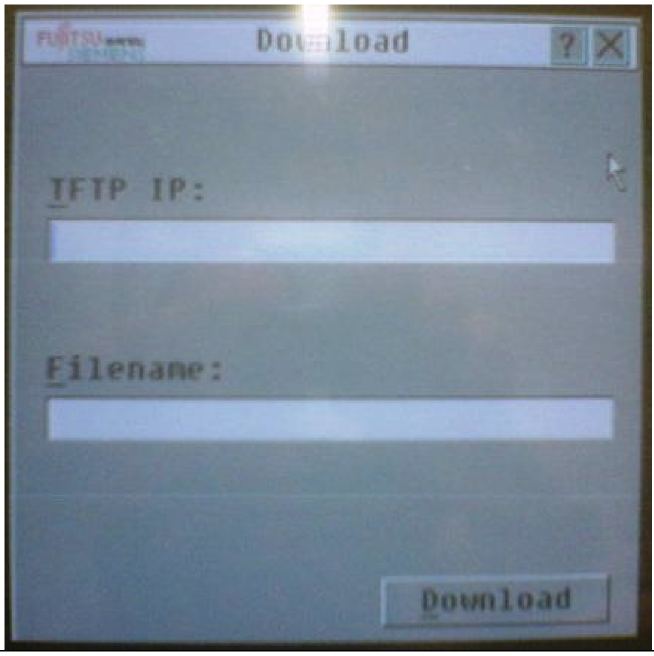
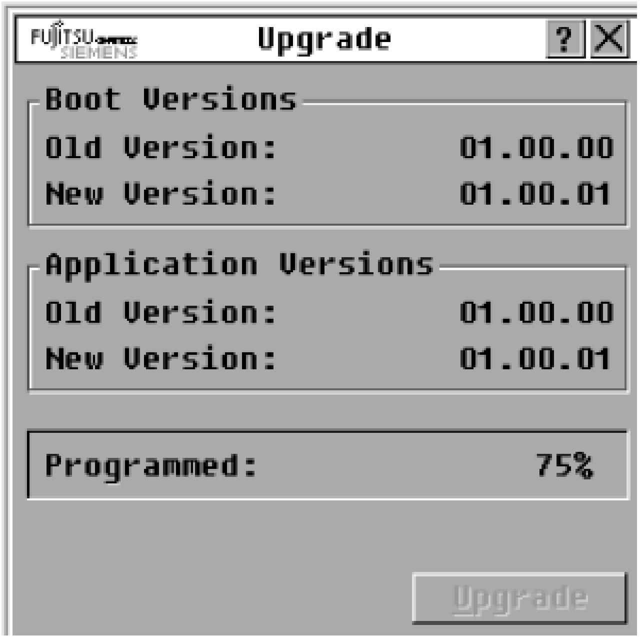
➢ Note: Use the **OSCAR** interface to view the firmware-version of the KVM s3-1621

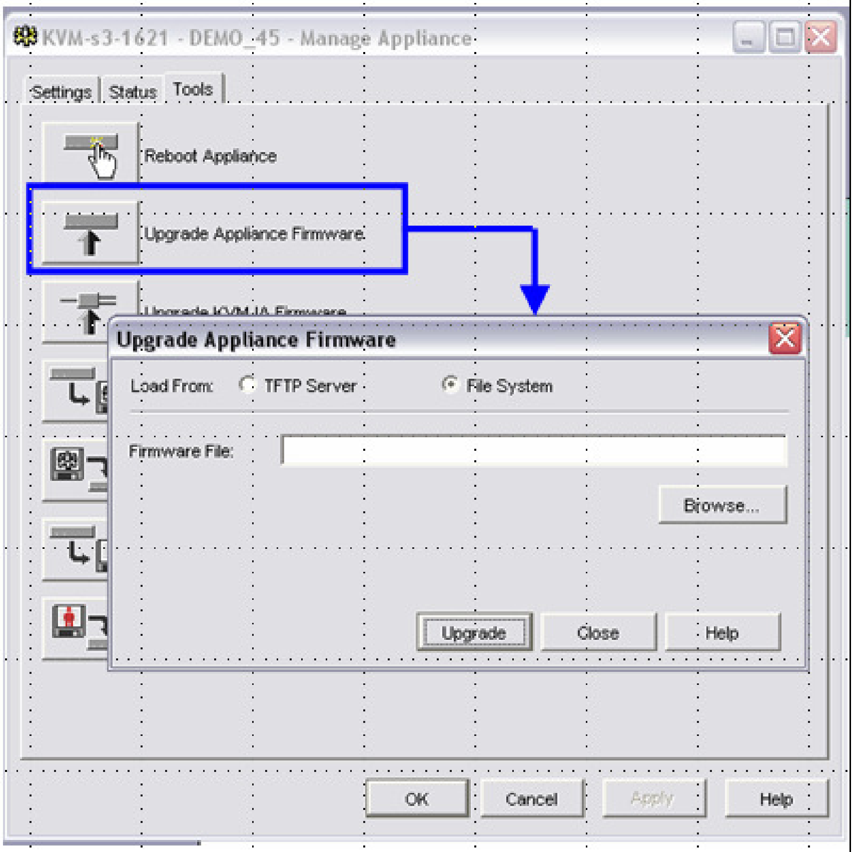
1. Press **Print Screen.** The Main window opens.
2. Click **Commands.** The Commands window opens.



3. Click **Display Versions.** The Version window opens.	
4. The top pane of the window lists the system versions in the KVM s3-1621 or KVM s3-1641 appliance. 5. Click **Upgrade**.	

9.3 Local Upgrading

6. Select the **source** of the new firmware file. 7. A **Warning** window opens. Click **OK.**	
8. The Upgrade window opens.	

9.4 Remote Upgrading	
• You can even use the **KVM s3 Client** to upgrade to a newer firmware version **remotely**.	

10 End of Exercise